REPORT DOCUMENTATION PAGE	*Form Approved* **OMB No. 0704-0188**

1. REPORT DATE *(DD-MM-YYYY)* 06-05-2012	**2. REPORT TYPE** Master of Military Studies Research Paper	**3. DATES COVERED** *(From - To)* September 2011 - May 2012

4. TITLE AND SUBTITLE
HARNESSING THE POWER OF INFLUENCE.

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Ansel, Justin J.

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
The globalized world offers unlimited ability to influence audiences around the world. We are currently engaged in a battle of perceptions and influence. The person or organization that achieves affects on its audience first will have more success. The advent of social media has compounded the targeted audience problem. Current doctrine defines roles and responsibilities that provide guidance in the information realm. The guidance provided does not allow for quick dissemination of ideas. The fear of misinformation (or propaganda) began immediately following World War II, with the Information and Exchange Act of 1948, more commonly known as the Smith-Mundt Act.

15. SUBJECT TERMS
Influence; social media; preceptions

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT** UU	**18. NUMBER OF PAGES** 36	**19a. NAME OF RESPONSIBLE PERSON** Marine Corps University / Command and Staff College
a. REPORT Unclass	**b. ABSTRACT** Unclass	**c. THIS PAGE** Unclass			**19b. TELEPONE NUMBER (*Include area code)*** (703) 784-3330 (Admin Office)

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at lest the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. 1F665702D1257.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234.

5d. PROJECT NUMBER. Enter al project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORS AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, VA 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

HARNESSING THE POWER OF INFLUENCE: WHY THE MARINE CORPS NEEDS TO COMBINE INFORMATION OPERATIONS AND PUBLIC AFFAIRS.

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Major Justin J. Ansel, USMC

AY 11-12

Mentor and Oral Defense Committee Member: Frank H. Marlo, Ph.D., Associate Professor of National Security Affairs

Approved: ______________________
Date: 3 May 2012
Oral Defense Committee Member: Paul Gelpi
Approved: ______________________
Date: 3 MAY 2012

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENT AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Executive Summary

Title: Harnessing the Power of Influence: Why the Marine Corps needs to combine information operations and public affairs.

Author: Major Justin J. Ansel, United States Marine Corps

Thesis: The Marine Corps needs to integrate Information Operations and Public Affairs to operate effectively in the globalized, fast-paced world.

Discussion: The idea of targeted audiences with specific messages is obsolete. The globalized world offers unlimited ability to influence audiences around the world. We are currently engaged in a battle of perceptions and influence. The person or organization that achieves affects on its audience first will usually have a more success. The advent of social media has compounded the targeted audience problem. Current doctrine defines roles and responsibilities that provide guidance in the information realm. The guidance provided does not allow for quick dissemination of ideas. The fear of misinformation (or propaganda) began immediately following World War II, with the Information and Exchange Act of 1948, more commonly known as the Smith-Mundt Act.

Today's information operating environment enables the war-fighter or supporter to participate at every level of influence operations. The intricate role that public affairs and information operations plays with the global reach of the internet or cyber domain offers an opportunity to quickly influence organizations and populations, targeted influence and general influence.

Conclusion: The Marine Corps public affairs personnel are uniquely suited to influence the Nation's adversaries. While there are those that disagree with combining the efforts, it is important that the Marine Corps remains relevant and effective in the information-operating environment.

Table of Contents

Page

Preface

With the prolific use of social media in today's operating environment, it is incumbent on our organizational leaders to understand and harness the power to influence. We stand at a unique intersection of a significant generational gap with technological experience and unparalleled ability to influence. The younger generation, the people/Marines/Sailors in today's armed forces have grown up and developed a greater intuitive understanding of this capability. This lack of understanding and clear contradiction of recognition of the potential to influence targeted audiences and organizations may cost the Marine Corps to lose the battle of perception. The fundamental lack of experience, education, and understanding of these concepts and how they relate to the operating environment and the US Constitution is the auspice of this paper. Excluding military deception and psychological operations, the ability to influence targeted population will become more important in the coming years.

I would like to thank all those who inspired and assisted me in this endeavor. The most prominent participant during the research was my MMS Mentor Dr. Frank Marlo; he directed my thoughts from a stream of conscience into a coherent, logical argument. Finally, I would like to thank my wife, Laura, for putting up with the long hours behind the computer researching and compiling my thoughts. She always provided relevant recommendations that helped me effectively communicate my thoughts.

"The future success of the Marine Corps depends on two factors: first, an efficient performance of all duties to which its officers and men may be assigned; second, promptly bringing the efficiency to the attention of the proper officials of the Government, and the American people."
- Major General John A. Lejeune, USMC, 13th Commandant

Information travels around the globe faster than ever before. The internet enables global influence and creates a fluid ever-changing information environment. The current construct of the Marine Corps' division of labor regarding information operations, public affairs and cyber, which are inextricably related, lacks the cohesion and responsiveness to incorporate or operate effectively to support mission commanders. The Marine Corps needs to integrate information operations and public affairs to operate effectively in the globalized, fast-paced world.

Long before globalization, General Lejeune addressed several aspects of today's information operating environment challenges. The Corps continues to struggle with the constraints within the information environment. "Efficient performance of all duties" is a key element of mission accomplishment. Publicizing the efficient performance of duties is standard fare for public affairs (PA). The accurate reporting conducted by public affairs has more influence around the world than commonly believed, "Promptly bringing" the information to not only the American people but also, more specifically, to those interested in the Marine Corps.[1]

The Marine Corps is less effective, due to the limitations within public affairs and information operations. The information-operating environment is a highly networked, internet-based, cyber dependant network that facilitates communication through a variety of different means. The transmission of information and the influence of ideas is so rapid the Marine Corps will constantly struggle to maintain an operational advantage. The Marine Corps established doctrine in maneuver warfare, which quickly determines the adversary's weakness and exploits that weakness. However, these current policies, by design, address nation states fighting with a uniformed military, distinct from the civilian population. Moreover, the current policies fail to address adequately groups or non-state actors.[2] As the world's population becomes increasingly urbanized, interconnected, and dependant on the internet, the lines blur even more. "The new definitions of warfare associate with complex environments, hybrid threats, transnational actors, dispersed operations, and the influence of tactical actions on strategic decision making could be argued to call for a much more prominent role for strategic communications (SC)."[3] To maintain the responsive nature of maneuver warfare the Marine Corps should recognize the changes in the information-operating environment associated with the probable conflicts and take the appropriate steps to continue to maintain an operational advantage.

The Threat and Problem Defined

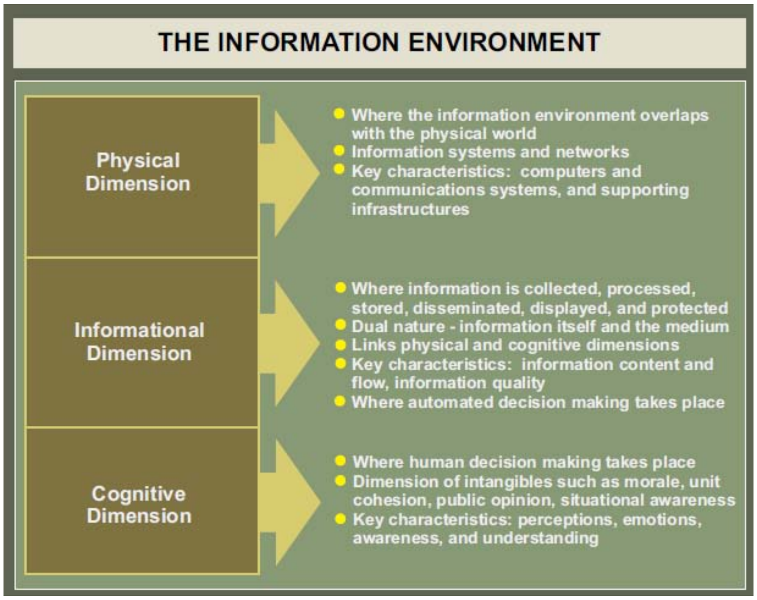
In today's operating environment, shaping operations commence long before the troops deploy or kinetic operations begin. Those shaping operations unfold as a battle of perceptions, ideas, and ultimately influence. The concept of information warfare is not new, in 1976; Thomas P. Rona first coined "information warfare", essentially stating that the information infrastructure was becoming a key component of the U.S. economy. "At the same time, it is becoming a vulnerable target in both war and peacetime."[4] He further stated the principal behind information warfare would become "a battle of decision systems."[5] For over thirty-five years, the United States, both in a military and a civilian capacity, has struggled to define information warfare and incorporate it into the decision cycle. The information-operating environment is more important today because of the capacity to influence in a globalized, inter-connected world.

Information is a broad term that encompasses many aspects; however, the Department of Defense (DOD) continues to wrestle with the definition. The latest attempt by the Marine Corps to define information operating environment is in MCWP 3-40.2 Information Management. "Information management – the processes, by which information is obtained, manipulated, directed, and controlled. IM includes all processes involved in the creation, collection and control, dissemination, storage and retrieval, protection, and destruction of information."[6] This definition considers information to be a quantifiable amount, limited to the consolidation of one person. The sheer amount of data and information that is available today has the potential to overwhelm individuals and organizations. MCWP 3-40.2 further defines an information system as "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[7] The idea that an information system can fit neatly into the description may have been possible prior to the advent of the internet but became obsolete with the advent of social networking sites.

The best definition of the information environment is from the IOsphere, a journal from the Joint Information Operations Center. This definition offers a holistic approach that includes the three dimensions of the IOE.

> The information environment is a construct based upon the idea that the existence and proliferation of information and information systems creates a distinct operating dimension or environment. As a combination of tangible (physical information systems and networks) and intangible elements (information and decision-making), the information environment is both a resource for military operations and a medium in which armed forces operate.[8]

Capturing the three elements of the definition enables a thorough understanding on the ability to manipulate influence across the domains; Figure 1 pictorially represents the information environment.



THE INFORMATION ENVIRONMENT

Physical Dimension

- Where the information environment overlaps with the physical world
- Information systems and networks
- Key characteristics: computers and communications systems, and supporting infrastructures

Informational Dimension

- Where information is collected, processed, stored, disseminated, displayed, and protected
- Dual nature - information itself and the medium
- Links physical and cognitive dimensions
- Key characteristics: information content and flow, information quality
- Where automated decision making takes place

Cognitive Dimension

- Where human decision making takes place
- Dimension of intangibles such as morale, unit cohesion, public opinion, situational awareness
- Key characteristics: perceptions, emotions, awareness, and understanding

Figure 1. The Information Environment (Source JP 3-13)

To operate effectively within the IOE there must be a common understanding of what is included in the IOE. As Figure 1 illustrates, the IOE is essentially anything that contains, transmits, or processes information. This may seem like an overwhelming amount of information; however, consolidating the ability to influence audiences within one organization would offer synergistic effects not realized currently. The IOE is constantly evolving. While the traditional means of transmitting information continues to exist in the form of newspapers, magazines, books, and established websites, it is important for commanders to understand the IOE is constantly changing and new communications systems affect the IOE. Command and control (C2) and decision-making information utilizes the electromagnetic spectrum, radio waves or fiber optic cables. The link between the informational and physical dimensions includes the internet or cyber sphere. This link allows the ability to influence on a global scale.

Physical Elements of the information-operating environment

Cyber as the Main Domain

The internet aligns closely with the "cyber domain" which must be considered simultaneously with IOE. The creation of the U.S. Cyber Command (USCYBERCOM) at Fort Meade, MD and the addition of service component equivalents is certainly progress, but there remains much consternation of what the cyber domain is, which has significant impacts on the division of responsibility within the IOE. The Department of Defense (DOD) and Marine Corps are already operating in the cyber domain and having effects in the IOE. However, unity of effort and focus of effort remain elusive. Joint Publication 3-13 defines cyberspace as the notional environment in which digitized information is communicated over computer networks, this definition originates from Joint Publication 1-02.[9] USCYBERCOM currently focuses efforts:

> USCYBERCOM will fuse the Department's full spectrum of cyberspace operations and will plan, coordinate, integrate, synchronize, and conduct activities to: lead day-to-day defense and protection of DOD information networks; coordinate DOD operations providing support to military missions; direct the operations and defense of specified DOD information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations. The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment.[10]

Rarely will a standalone network be completely secure from an interconnected network, the internet. Cyberspace took twenty years to become part of the military vernacular, and now permeates every aspect of the IOE and command and control (C2). Establishing USCYBERCOM is the first step in recognizing the importance and the impact that the cyber domain has during military operations. When considering the IOE, one must include the cyber domain to remain relevant.

Because of the emphasis the U.S. government has put on the cyberspace domain environment it is incumbent the Marine Corps continues to develop and refine policies and procedures to address the IOE, specifically elements from cyberspace.

> Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people. As Internet usage continues to expand, cyberspace will become increasingly woven into the fabric of everyday life across the globe.[11]

The cyber domain is part of the physical dimension, and the information contained in that domain falls within the informational dimension. This information contains social networking sites, which play an important role in the dissemination of information dimension. There is a significant generational gap in understanding and employment of social media. "I'll Facebook you" – that term is heard by millions of people today. Social media plays such an integral role in daily lives that the older generation, today's mid-level and executive managers (or leaders). Executive leaders are required to understand the influence of SNS on the individuals within an organization, despite the purpose of the organization or mission. These leaders must be able to effectively communicate with subordinates and effectively utilize the spectrum of social media, which possess a significant amount of power to influence with military application. This understanding is significant when considering the intimate relationship social media plays with cyber operations, which as Figure 1 denotes is part of the physical dimension of the information-operating environment.

Current Doctrine

Joint Publication 3-13 (JP 3-13), Information Operations, defines information operations (IO) as having five core competencies: psychological operations, military deception, operations security, electronic warfare, and computer network operations. A consistent theme of the five IO core competencies is the ability to influence. JP 3-13 essentially associates IO with influence on the adversary, while public affairs tend to serve friendly forces or the public perception. The globalized nature of today's IOE and communication abilities hampers the ability to limit information to a targeted audience. For example, the intended target may be an adversary, but the potential for friendly forces to be influenced is greater today because of the interconnected information systems. This is where the current doctrine lacks flexibility.

The Smith-Mundt Act

The source of the inflexibility is the Information and Exchange Act of 1948, more commonly known as the Smith-Mundt Act, which countered the misinformation of the communists immediately following World War II. However, the United States government (USG) was concerned about the State Department, and ultimately the military inappropriately influencing the American people or the communist influence spreading abroad and at home. The USG needed a way to spread the good story about democracy and the United States. The Smith-Mundt Act accomplished three major protections. First, it maximized the use of private media. Second, the new law ensured the State Department would not monopolize broadcasting, which occurred in Nazi Germany and the Soviet Union. Finally, the Smith-Mundt eliminated the ability for the State Department to broadcast domestically; a concern that the State Department would exert influence over the American people.[12] The access to information during this time was limited to print media, radio, and direct communications between individuals; not the complex interconnected internet; traditional media was easier to control.

Today the availability to present information allows an unprecedented ability to influence. The current IOE enables individuals to influence groups and organizations more efficiently today than in 1948. However, the importance of efficiently communicating a message that counters ideals contrary to democratic values is more important than restricting the ability to affect this influence.

Determine Friend or Foe

The ability for the Marine Corps to influence its members is the responsibility of public affairs; however, the influence, more often than not, extends beyond the intended audience. Focusing efforts to maintain pace with the news cycle is necessary and pushing the release authority to the lowest level possible would facilitate a more effective approach, regardless of the intended audience. The cyber domain inextricably ties information-operating environment to the domestic and foreign audiences, which presents a unique challenge to limit exposure to unintended audiences.

Methods of Influence

Success within the information-operating environment predicates the ability to operate unimpeded throughout the cyber domain and the incorporate the informational dimension. A stark absence from JP 3-13 is the ability to shape the information-operating environment. Social networking sites offer the ability to influence a wide audience through the cyber domain. Often times Information Operations and Strategic Communications can make the difference in mission accomplishment. Weakening an adversary's will to fight or to influence decisions through the internet is possible with effective targeting of the adversary's cognitive dimension.

The internet offers opportunities to influence large audiences at any given time. There are more social media sites in 2012 than ever before. The multitude of venues offered by social media sites, organizations, employers, or startups grows every day. There is a new approach that one organization takes which may or may not take root and grow. The types of social media are as diverse as the imagination and may include blogs, wikis, micro-blogs, social networking sites, video/photo sharing websites, forums, message boards, user-generated content, and text message services. All of these venues offer a great deal more versatility than average voice communications.

More intrusively, mobile computing devices allow for a greater degree of access which complicates the matter with instant access to the global information grid (GIG). Specifically, smart phones have enabled the use of social media to the point where it is impossible to navigate industry or profession while avoiding its use. The Marine Corps struggled with the correct approach to social media, as noted by the temporary ban on social media in 2009.

The concern of the Marine Corps is the inappropriate use of social media sites. The knee jerk reaction of MARADMIN 0458/09, called for an immediate ban of internet social networking sites (SNS) on the Marine Corps Enterprise Network (MCEN).[13]

> Internet SNS are defined as web-based services that allow communities to people to share common interests and/or experiences …. These Internet sites in general are a proven haven for malicious actors and content and are particularly high risk due to information exposure, user generated content and targeting by adversaries. The very nature of SNS creates a larger attack and exploitation window, exposes unnecessary information to our adversaries and provides an easy conduit for information leakage that puts OPSEC, COMSEC, personnel and the MCEN at an elevated risk of compromise.
>
> Access is hereby prohibited to internet SNS from the MCEN NIPRNET.[14]

The Marine Corps quickly realized the difficulty with banning access to social media throughout the work place and reversed the decision.

This temporary ban enabled the Marine Corps to reduce the risk associated with SNS as requested by US STRATCOM, the agency originally responsible for the cyber domain. In contrast, other companies, like Haliburton Country Development Corporation, offer social media boot camps or a place to learn how to navigate through the complicated web of traps, "It's ideal for individuals, organizations, and non-profits interested in using social media to engage, communicate and create change."[15] Haliburton's approach may serve as an example to the Marine Corps and other government agencies.

Although entities utilize social media to initiate change, there are several examples in recent history that provide insight on how to use social media effectively as a means to coordinate these efforts: the Arab Spring, the London riots, and the Occupy movement in the United States. On the anniversary of the collapse of the Egyptian government, one that lasted over 40 years, several entities have had sufficient time to study the influence social media played on organization, dissemination, and overall effectiveness of the movements. In the case of the Arab Spring,

> After analyzing more than 3 million tweets, gigabytes of YouTube content and thousands of blog posts, a new study finds that social media played a central role in shaping political debates in the Arab Spring. Conversations about revolution often preceded major events, and social media has carried inspiring stories of protest across international borders.[16]

The effectiveness of these movements and the influence over a group of people is profound. While social media did not cause the revolution, it allowed the revolution to organize, largely through social media.

The London riots had a markedly different purpose than the Arab Spring. While the Arab Spring attempted to bring about democratic change, the London riots brought about organized chaos, for the purpose of rioting and looting. The movement, which ignited with the alleged unprovoked shooting of a black teenager by a white police officer, was more of a release of frustration and an excuse to conduct mischievous acts under the guise of protests. The primary medium in this case was not Facebook, but Blackberry mobile phones, specifically the messenger application. Interestingly, the same tools that brought the violence also brought about restitution.[17] Many counter-riot individuals organized the cleanup efforts that were able to clean the areas affected by the riots and returned property to its rightful owners.

Finally, the third comparison for social media as an organizational tool is the Occupy Wall Street movement. While the desires of the protest are to encourage a better understanding of how the top one percent of society is taking advantage of the rest of the country, it has largely been peaceful, passive demonstrations. The movement continues to maintain its strength through the interconnectedness of social media, "Social media sites such as Facebook and Twitter have been central organizing locations for spreading information about Occupy Wall Street."[18] Protestor's blogged and coordinated efforts through computers while participating in the actual protest.

These are clear examples of social media organizing efforts to achieve a certain result – accomplish a mission. The physical means of transferring information used during these three movements all incorporated some aspect of social media. The command and control of these distinct operations would be challenging for the most proficient military unit. However, untrained, young people – motivated by a cause – are effortlessly accomplishing this on a daily basis. This type of organizational leadership is directly transferrable to purposeful organizations, as long as the leader understands how to navigate through the social media maze within the IOE.

The intersection of informational and physical dimension is the internet. With the amount of data available to the individual, organization, or government it is possible to collect and use data to coordinate actions or for military applications. The physical dimension of the information environment offers an opportunity to exploit unsecured mediums and isolate adversaries from command and control nodes. Ultimately, the ability to control the physical dimension will have profound influence on the decision-making abilities of the adversary. "Possible threat information techniques include, but are not limited to, deception, electronic attack (EA), computer network attack (CNA), propaganda and psychological operations, and supporting signals intelligence (SIGINT) operations."[19] Consideration for the vulnerability of the information-operating environment and the method of information transfer should factor into the decision-making process.[20]

Future Applications of Influence

As the social media phenomenon continues and the idea of a true social network matures, the military applications to influence are unlimited. A small organization of highly skilled individuals with unlimited amount of references at their disposal could achieve strategic results, if employed effectively. Operating within a social network with the ability to address aspects of a certain environment in real time is a possibility. The ability to provide a collaborative network synthesizing open source intelligence with classified intelligence would allow decisions that are more effective and increase an individual's ability to process detailed information. Much like the virtual private network (VPN) on a smart phone, a Marine could have a heads up display and would be able to see improvised explosive device hotspots, labeled compounds of known adversaries, old weapons caches, or anything else pertinent to the mission.

While the applications are plentiful, there are pitfalls. In order to operate effectively within the IOE, internet connectivity is necessary. With any network come the associated risks of cyber war, CNO, CND, and CNE. Building a base of knowledgeable practitioners with education and training is expensive and time consuming; however, training a base of support with experience would enable true proficiency in this domain. The underlying concern is that it may be too late before the Marine Corps identifies the right way forward.

Recently, U.S. Special Operations Command (USSOCOM) disclosed that, they are attempting to produce a new type of social media, one that would allow the users to provide immediate feedback to television and radio broadcasts. [21] This feedback mechanism would provide a response indicator to gauge the effectiveness of targeted information operations. The challenges associated with USSOCOM operating in such austere locations without the luxury of an interconnected society make it difficult to achieve immediate results. USSOCOM is attempting to provide the technology to the population that they are attempting to influence in order to meet the needs of the system.[22]

The Information Operating Environment and the Cognitive Dimension

Given that SNS are becoming increasingly important in the daily operations of many organizations and individuals, there are new technologies that are capable of influencing public opinion, which the Marine Corps should embrace. Theorists, like Shen Weiguang, are embracing the potential efforts within the information-operating environment.[23] The ability to influence can have profound impacts on military and political objectives.

A well-executed campaign, in the information-operating environment, can have immediate, decisive effects. The Israeli-Hezbollah War of 2006 provides significant insight to the effective use of the information-operating environment. "Nik Gowing, a respected BBC world anchor, warned at a recent Harvard conference that the 'new asymmetric information' – the new level of accountability and public perceptions in a time of crisis exposed the vulnerability of traditional institution of power and influence."[24] The ability of the Hezbollah to release information quickly to influence public opinion was not constrained by restrictions on the intended targeted audience. The images displayed in real time through the physical dimension produced distinctive cognitive affects of the viewers.

Russia made tremendous progress in the information-operating environment during the 2008 short war with Georgia. While operations in the IOE take many forms, the Russians chose elements from the higher end of the IOE, i.e. offensive cyber operations, isolation of a country, and conventional military operations. By isolating the Georgian C2 ability, the Russians were effectively able to dominate the IOE. The Russian influence slanted the news coverage to portray Georgia as the aggressor. Thus, the actual effects of the Russian success in the IOE were in the perceptions of those watching the news (informational dimension) and the impressions the news left them with (cognitive dimension).[25]

Organizations and individuals make decisions based on the information available. The information and influence from the internet, specifically SNS, is plentiful. In a normal decision cycle, information is input to the system, the organization or individual then processes that information and, eventually coming to a conclusion. Today the availability of information and direction of the influencers are so immense that Marine Corps models of decision-making do not account for the complex operating environment of the IOE. JP 3-13 explained the information environment, Figure 2 graphically represents the decision cycle with influence inputs as it lies over physical aspects of the IOE.

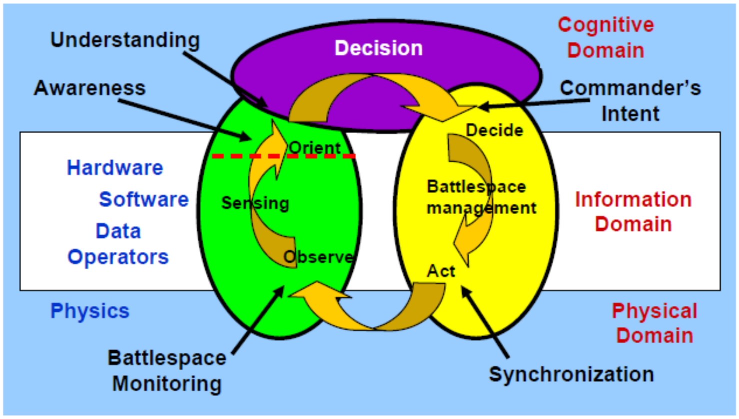


Figure 2
The Decision Cycle within the IOE

Whether a standard SNS or a lesser-known blog, information is produced faster than most organizations including the Marine Corps can keep pace. The Marine Corps does not currently possess the ability to respond to this amount of information in a decisive manner. The most important aspect within the cyber domain is people, but the Marine Corps' latest technology cannot defeat the action of users, whether unintentionally or purposefully malicious.

Revising the Smith-Mundt Act

While the concern of crossing inappropriate influence from the government to the American population is valid, in today's interconnected information environment influence is expected. The information-operating environment continues to evolve and the USG should update the Smith-Mundt Act to provide the Marine Corps the ability to utilize the latest technologies to maintain a cohesive organization. The consideration of influence in a democratic society can be balanced with civilian oversight. Civilian oversight and government transparency is necessary when approaching this problem. Immediately following the London riots, the overwhelming majority considered the blocking of social networks a proper course of action.[26] Several months prior to the riots, the Egyptian government attempted to shut down the internet, thinking that would eliminate the protest, or at least keep them at a manageable level.

Updating the Smith-Mundt would allow the efforts of not only the private news media outlets but also the government, namely the DOD, to influence a targeted audience more effectively. The combination could potentially assist the war-fighter with effective influence over an adversary. While the USG updates laws, the Marine Corps, by combing public affairs and information operations efforts, could become a more effective organization.

Leading individuals and organizations in IOE

In order to operate effectively within the social realm, organizational leaders must determine what is best for their organization. The idea that any organization can be effective by eliminating individuals from participating in social media is unrealistic. As seen in the Haliburton Country Development Corporation example, executive leadership educated the members of their organization and trusted them to operate effectively within the informational dimension. This approach may initially draw criticism and the long-term gain may take some time to realize, but Haliburton's success serves as an effective model.

Training, education, and leadership are the tools required for effective operations within the Information Operating Environment. However, organizations consist of individuals that normally work together to accomplish a mission, while abiding by the organization's guiding principles. Regardless of the technological advances or latest security measures, the individual is expected to practice good, disciplined application of proper security procedures. Despite the latest technological safeguards, Bradley Manning stole a tremendous amount of data from his workstation, where he possessed unfettered access to information. Leading Marines through the information environment takes more than technology; it requires the same ethos as leading Marines into battle. The insider threat is, and will remain the single largest threat to any network and can have catastrophic effects on the decision-making or cognitive dimension of the organization, the public and the adversary.[27]

Effective operations within the IOE result in decisive effects in the cognitive dimension of the intended target, whether friend or foe. However, to achieve desired effects at a decisive moment, the commander must understand the group and individual decision cycles and the influential aspects of the information-operating environment. Figure 3 displays the current conceptual decision cycle of an organization. Ultimately, the commander makes a decision, but the influence throughout the decision cycle determines the outcome of the decision. This is the purpose of the information-operating environment: to affect the individuals or groups making decisions. Absent from Figure 3 are the influencers that affect each step of the cycle.

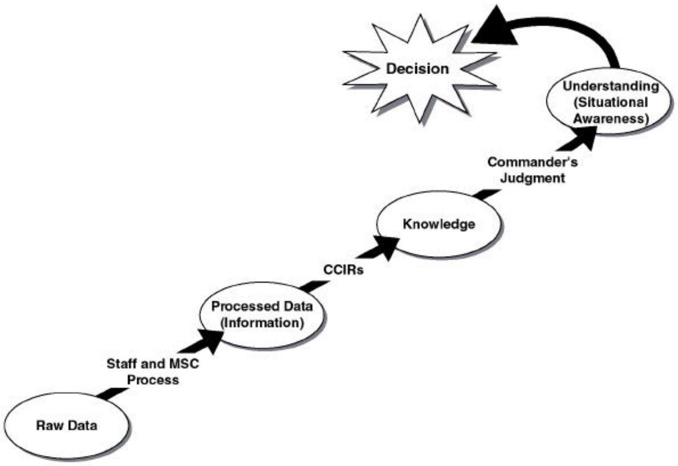


Figure 3. The Decision Cycle

Examples of Effective Influence through Social Media

Most notably, groups and individuals effectively employed messages during the Arab Spring in 2011. While the actual catalyst remains uncertain, there is little doubt that operations in the information environment played an important role in spreading and fueling the revolts. Like-minded individuals were able to coordinate efforts, share ideas, and take action. Anonymous individuals' coordinated the protests from the security of their homes, "A spike in online revolutionary conversations often preceded major events on the ground."[28] Coordination in relative security empowered large numbers of people to protest at the same time. The confidence gained from the online revolutionary discussions spread faster than existing governments could handle. Democratic advocates "By using digital technologies…created a freedom meme that took on a life of its own and spread ideas about liberty and revolution to a surprisingly large number of people."[29] Despite efforts to shut down websites or limit access to the internet, those operating effectively within the IOE established websites outside of the area of governmental influence. For example, "The Muslim Brotherhood relied on bloggers whose servers were located in London and therefore couldn't be taken offline."[30] While the Muslim Brotherhood is not a pro-democracy organization, they used a democratic process of protests to rise to power. The population using social media was susceptible to the influence of a compelling message. Individuals and groups successfully exploited opportunities to influence which resulted in an increased participation of the Arab Spring.

David Kilcullen spoke of the Taliban's prowess in the IOE throughout the Helmand Province. The Taliban will determine the influence (cognitive) desired on a population, then plan events to support that message. On the contrary, US forces typically utilize post-event planning to achieve results in the cognitive dimension.[31] The fact that it frequently takes time to issue the message raises the question of whether operations should drive what a commander is attempting to influence or whether the message should drive the operations of the commander. Clearly, Shen Weiguang and the PRC perceive influence as the most important aspect of operations.[32]

Effectively Operating within the Current Systems

Because command and control executed within the information-operating environment, it is necessary to incorporate the IOE into existing Marine Corps concepts. As depicted in Figure 4, influence can occur during any element of the command and control model. “Marine Corps warfighting functions encompass all aspects of military activities that occur during operations. Planners consider and integrate the warfighting functions when determining how to accomplish a mission. Integrating the warfighting functions ensures an integrated plan and helps achieve unity of effort and focus throughout the mission.”[33] The Information Operating Environment fits squarely into the existing six war-fighting functions. Clearly, the IOE encompasses elements of the command and control, intelligence, fires, logistics, and force protection, whether in the literal or the figurative sense. The remaining war-fighting function, maneuver, is a bit more ambiguous when dealing with the IOE; however, gaining a position of advantage with respect to the enemy can take on many forms, linear or asymmetric. Exploiting the cognitive dimension to gain a position of advantage is certainly possible, as seen in the Arab Spring.

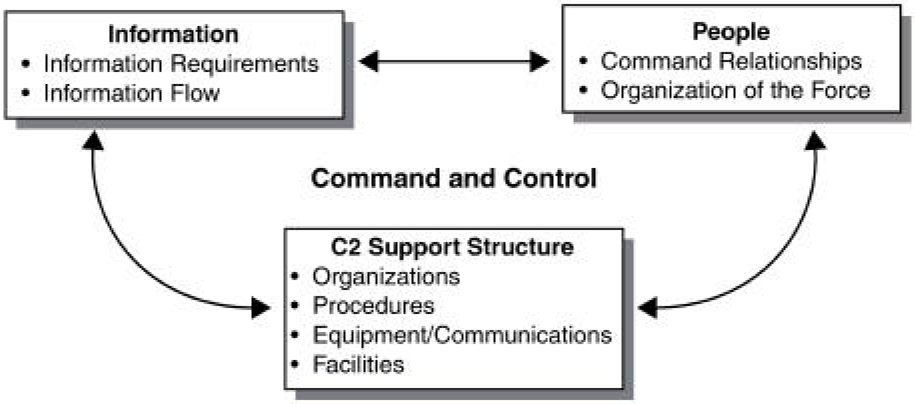


Figure 4.

Elements of Command and Control

Requirements for Change

As the information domain continues to expand, the urgency for understanding how to operate within it is a necessity. Combining the public affairs and information operations to account for globalization is forward progress. Effective media campaigns will combine the information domain with tangible effects, in fact, mastering the IOE could lead to adversary's capitulation before hostilities commence. Operations in the information operating environment and effects in cyberspace will drive mission accomplishment. Incorporating a more effective doctrine, which enables commanders to effectively employ non-kinetic influence, will directly affect the need for kinetic operations. The sooner the Marine Corps combines aspects of the information-operating environment -- information operations, strategic communications, and pubic affairs -- the more efficient the influence will become.

Possessing expertise in the IOE would allow a more efficient mapping of the IOE. "Visualization of the information environment and its effects on military operations is essential to planning and executing an information operation."[34] The ability to influence a targeted audience is becoming more important as the population becomes dependant on networks to communicate. Successful operations may be limited to a comprehensive information campaign, which targets the cognitive dimension of the adversary. Until the Marine Corps adjusts the current approach to information operations, strategic communications, and public affairs, commanders will operate at a disadvantage against adversaries.

Conclusion/Recommendations

Influencing individuals, organizations, or an adversary is the intent of operations within the IOE. The Marine Corps public affairs personnel are uniquely suited to accomplish this.

With minor adjustments, they can operate more effectively in the information-operating environment, by combining efforts between traditional and nontraditional media outlets. However, the primary change is the using the individual Marine, with permissive oversight, as the principal spokesperson for the Marine Corps. As technology progresses and information sharing improves, the Marine Corps must continue to streamline operations in the IOE.

The adversaries of the future will continue utilizing the IOE to influence a targeted population. Future conflict will be unrecognizable by today's standards and will require an improved understanding of maneuver warfare in unconventional environments, such as the IOE. If utilized properly, influence operations may lead to capitulation by the adversary before the opening salvos of kinetic operations. The goal of influence operations within the IOE is to "render the enemy incapable of resisting effectively by shattering his moral, mental, and physical cohesion."[35] The great Chinese philosopher of war, Sun Tzu, stated, "One hundred victories in one hundred battles, is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[36]

computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

computer network defense. Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called CND. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1- 02.)

computer network exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE. (Approved for inclusion in the next edition of JP 1-02.)

computer network operations. Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. (Approved for inclusion in the next edition of JP 1-02.)

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy’s effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)

Global Information Grid. The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services and National Security Systems. Also called GIG. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 6-0.)

information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

military deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces mission. Also called MILDEC. See also deception. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-58.)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (JP 1-02)

public affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA. (JP 1-02)

strategic communication. Focused United States Government (USG) efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power. (Approved for inclusion in the next edition of JP 1-02.)

target audience. An individual or group selected for influence. Also called TA. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

Bibliography

Ansel, Justin, Larry Fletcher, and Geoffrey Gorsuch, “Military Applications in Social Media.” Manuscript, Command and Staff College, Marine Corps University, 2012.

Armstrong, Matt, “Rethinking Smith-Mundt,” *Small Wars Journal,* (July 2008)

Ball, James, “Two-thirds support social networking blackout in future riots.” The Guardian, November 7, 2011. http://www.guardian.co.uk/media/2011/nov/08/two-thirds-support-social-media-blackout (Accessed January 24, 2012).

Baker, Ralph O. Brigadier General Ralph, US Army, “Information Operations, From Good to Great.” *Military Review*, (July-August 2011): 2-7.

Berkowitz, Bruce. *The New Face of War: How war will be fought in the 21st century*. New York, Simon & Schuster, Inc. 2003.

Caren, Neal and Sarah Gaby, “Sociologist Tracks Social Media’s Role in Occupy Wall Street Movement.” Working paper, Department of Sociology, University of North Carolina, February 21, 2012.

Carr, Jeffery. *Mapping the Cyber Underworld, Inside Cyber Warfare.* California, O’Reilly Media, Inc., 2010.

City, Panama, Pan American Publishing Company, 2002Thomsen, Brian M., Haney, Eric L. ed. *Beyond Shock and Awe, Warfare in the 21st Century.* New York, Penguin Group Inc., 2006.

Cordary III, Robert and Romanych, Marc J., “Mapping the Information Environment.” *IOSphere, Joint Information Operations Center*, (Summer 2005): 7-10.

Commandant of the Marine Corps. *Immediate Ban of Internet Social Networking sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET.* MARADMIN 458/09. http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx (accessed 24 January 24, 2102).

Clarke, Richard A. and Robert K. Knake. *Cyber War, The Next Threat to National Security and What to do about it.* New York: HarperCollins Publishers, 2010.

Clausewitz, Carl von. *On War*. Edited by Michael Howard and Peter Paret. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Emery, Norman, D.G. Mowles, Jr., and Jason Werchan , “Information Operations Doctrine and Non-state Conflict: Shaping the Information Environment to Fight Terrorism and Insurgencies.” *IOSphere, Joint Information Operations Center*, (Spring 2005): 7-13.

Farwell, James, “The Emerging Battlespace of Cyberwar: The Legal Framework and Policy Issues.” *IO Journal*, Vol. 1, (February 2010): 12-20.

Gray, Colin S. *Another Bloody Century, Future Warfare*. London: Orion Publishing Group, 2005.

Haliburton Country Development Corporation, http://www.haliburtoncdc.ca/events-seminars-training/events/social-media-bootcamp.html (Accessed January 24, 2012).

Headquarters U.S. Marine Corps. *Information Management.* MCWP 3-40.2. Washington, DC: Headquarters U.S. Marine Corps, January 24, 2002.

Headquarters, United States Marine Corps, *Marine Air-Ground Task Force Information Operations*, MCWP 3-40.4, Washington, DC: Headquarters US Marine Corps, July 9, 2003.

Headquarters U.S. Marine Corps. *Marine Corps Planning Process.* MCWP 5-1. Washington, DC: Headquarters U.S. Marine Corps, August 24, 2010.

Headquarters U.S. Marine Corps. *Warfighting.* MCDP 1. Washington, DC: Headquarters U.S. Marine Corps, June 30, 1991.

Hollis, David, “Cyberwar Case Study: Georgia 2008”, *Small Wars Journal,* (January 2011), 1-10.

Howard, Philip N., Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. “Opening Closed Regimes,” Working paper 2011.1, Project on Information Technology & Political Islam, http://www.scribd.com/doc/66956384/Opening-Closed-Regimes (Accessed 24 January 24, 2012).

Iyer, Prem, “Where is your biggest threat? Look inside the enterprise.” High Tech Highway, January 24, 2012 http://www.hightech-highway.com/secure/where-is-your-biggest-threat-look-inside-the-enterprise/ (Accessed February 18, 2012).

Johnston, Hank, ed. *Culture, Social Movement and Protest.* Great Britain, MPG Books, Ltd., 2009.

Jones, Kemper, telephone conversation with author, January 17, 2012.

Josten, Richard J., “Strategic Communication: Key Enabler for Elements of National Power.” *IOSphere, Joint Information Operations Center*, (Summer 2006): 16-20.

Kalb, Marvin, “The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict.” *John F. Kennedy School of Government – Harvard University*. Faculty Research Working Papers Series, RWP07-12, February 2007.

Kelley, Olen L. Colonel, “Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative.” Master’s Thesis, U.S. Army War College, 2008.

Kosar, Kevin R. *Public Relations and Propaganda: Restrictions on Executive Agency Activities.* CRS Report for Congress RL32750. Washington, DC: Congressional Research Service, March 21, 2005.

Lenkart, John J., “The Vulnerability of Social Networking Media and the Insider Threat: New Eyes for Bad Guys.” Master’s Thesis, Naval Postgraduate School, September 2011.

Marine Corps Functional Concept for Strategic Communications (SC), *Marine Corps Operating Concepts*, Third Edition, (June 2010): Appendix A.

Polania, William G., “Leveraging Social Networking Technologies: An Analysis of the Knowledge Flows Facilitated by Social Media and the Potential Improvements in Situational Awareness, Readiness, and Productivity.” Master’s Thesis, Naval Postgraduate School, September 2010.

Qiao Liang and Wang Xiangsui. *Unrestricted Warfare: China’s Master Plan to Destroy America*. Panama, 2001.

Sentse, Rob and Storm, Arno, Majors Royal Netherlands Army, “The Battle for the Information Domain.” *IO Journal*, Vol. 1, (February 2010): 5-11.

Shachtman, Noah, “Special Forces Get Social in New Psychological Operation Plan.” Wired, January 20, 2012. http://www.wired.com/dangerroom/2012/01/social-network-psyop/ (Accessed January 24, 2012).

Shapiro, Andrew L.. *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know.* New York, Public Affairs TM, 1999.

Shirky, Clay. *Cognitive Surplus, Creativity and Generosity in a Connected Age*. New York, The Penguin Press. 2010.

Stepanova, Ekaterina, “The Role of Information Communication Technologies in the ‘Arab Spring’ Implications Beyond the Region.” PONARS Eurasia Policy Memo No. 159, (May 2011).

Tzu, Sun. *The Art of War*. Edited by Samuel B. Griffith. Translated by Samuel B. Griffith. New York, Oxford University Press, 1963.

U.S. Department of Defense, *U.S. Cyber Command Fact Sheet*, U.S. Department of Defense Office of Public Affairs. Arlington, VA: Department of Defense, 2010.

U.S. Joint Chiefs of Staff. *Information Operations.* Joint Publication 3-13. Washington, DC: Headquarters U.S. Joint Chiefs of Staff, February 13, 2006.

Wasik, Bill. “#Riot: Self-Organized, Hyper-Networked Revolts – Coming to a City Near You.” *Wired*, December 16, 2011. Wired January 2012.

Wicks, Robert H., *Understanding Audiences: Learning to Use Media Constructively*. New Jersey, Lawrence Erlbaum Associates, 2001.

Winchester, Regina S. Major USAF, “Strategic Communication and Public Affairs: Training Today for the Future.” Master’s Thesis, Air Command and Staff College, Air University, 2008.

[1] Those that support or have a stake may include Marines, families of Marines, local business near Marine Corps bases, coalition partners, other government agencies and finally - adversaries and potential adversaries.

[2] Information Operations Doctrine and Non-state Conflict: Shaping the Information Environment to Fight Terrorism and Insurgencies, by Norman Emery, D.G. Mowles Jr., Jason Werchan, IO Sphere, Joint Information Operations Center, Spring 2005

[3] The Marine Corps Functional Concept for Strategic Communications (SC), 13

[4] Lin, Abe C. General, *COMPARISON OF THE INFORMATION WARFARE CAPABILITIES OF THE ROC AND PRC*, Dec 2000.

[5] Thomas P. Rona, "Weapon Systems and Information War", Boeing Aerospace Co., Seattle, WA, 1976

[6] Headquarters U.S. Marine Corps. *Information Management,* MCWP 3-40.2. (Washington, DC: Headquarters U.S. Marine Corps, January 24, 2002), 6.

[7] Headquarters U.S. Marine Corps. *Information Management,* MCWP 3-40.2. (Washington, DC: Headquarters U.S. Marine Corps, January 24, 2002), 8.

[8] Mapping the Information Environment**,** *By Robert Cordray III, Marc J. Romanych, Major, USA (Retired)*

[9] U.S. Joint Chiefs of Staff. *Information Operations.* Joint Publication 3-13. (Washington, DC: Headquarters U.S. Joint Chiefs of Staff, February 13, 2006), GL-6.

[10] U.S. Department of Defense, *U.S. Cyber Command Fact Sheet,* U.S. Department of Defense Office of Public Affairs. Arlington, VA: Department of Defense, 2010.

[11] Department of Defense Strategy for operating in Cyberspace, July 2011

[12] Matt Armstrong, "Rethinking Smith-Mundt," *Small Wars Journal,* (July 2008).

[13] Commandant of the Marine Corps. Immediate Ban of Internet Social Networking sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET, MARADMIN 458/09, August 3, 2009. http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx (accessed 24 January 24, 2102).

[14] Commandant of the Marine Corps. Immediate Ban of Internet Social Networking sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET, MARADMIN 458/09, August 3, 2009. http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx (accessed 24 January 24, 2102).

[15] Haliburton Country Development Corporation, http://www.haliburtoncdc.ca/events-seminars-training/events/social-media-bootcamp.html (Accessed January 24, 2012).

[16] Science News, New Study Quantifies Use of Social Media in Arab Spring**,** *ScienceDaily (Sep. 14, 2011)*

[17] Erica Swallow, London Riots: Social Media Mobilizes Riot Cleanup August 09, 2011

[18] Neal Caren, "Sociologist Tracks Social Media's Role in Occupy Wall Street Movement." (working paper, Department of Sociology, University of North Carolina, 2012).

[19] U.S. Joint Chiefs of Staff. *Information Operations.* Joint Publication 3-13. (Washington, DC: Headquarters U.S. Joint Chiefs of Staff, February 13, 2006), pg I-5, I-6.

[20] Justin Ansel, Larry Fletcher, and Geoffrey Gorsuch, "Military Applications in Social Media." (Manuscript, Command and Staff College, Marine Corps University, 2012).

[21] Noah Shachtman, "Special Forces Get Social in New Psychological Operation Plan." Wired, January 20, 2012, http://www.wired.com/dangerroom/2012/01/social-network-psyop/ (Accessed January 24, 2012).

[22] Noah Shachtman, "Special Forces Get Social in New Psychological Operation Plan." Wired, January 20, 2012, http://www.wired.com/dangerroom/2012/01/social-network-psyop/ (Accessed January 24, 2012).

[23] Norman Emery, D.G. Mowles, Jr., and Jason Werchan , "Information Operations Doctrine and Non-state Conflict: Shaping the Information Environment to Fight Terrorism and Insurgencies." *IOSphere, Joint Information Operations Center*, (Spring 2005): 9.

[24] The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict, Marvin Kalb, February 2007

[25] David Hollis, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal,* (January 2011), 1-10.

[26] James Ball, “Two-thirds support social networking blackout in future riots.” The Guardian, November 7, 2011. http://www.guardian.co.uk/media/2011/nov/08/two-thirds-support-social-media-blackout (Accessed January 24, 2012).

[27] Prem Iyer, “Where is your biggest threat? Look inside the enterprise.” High Tech Highway, January 24, 2012 http://www.hightech-highway.com/secure/where-is-your-biggest-threat-look-inside-the-enterprise/ (Accessed February 18, 2012).

[28] Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. “Opening Closed Regimes,” *Project on Information Technology & Political Islam*, Working paper 2011.1, January 2011, 1, http://www.scribd.com/doc/66956384/Opening-Closed-Regimes (Accessed 24 January 24, 2012).

[29] Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. “Opening Closed Regimes,” *Project on Information Technology & Political Islam*, Working paper 2011.1, January 2011, 3, http://www.scribd.com/doc/66956384/Opening-Closed-Regimes (Accessed 24 January 24, 2012).

[30] Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. “Opening Closed Regimes,” *Project on Information Technology & Political Islam*, Working paper 2011.1, January 2011, 3, http://www.scribd.com/doc/66956384/Opening-Closed-Regimes (Accessed 24 January 24, 2012).

[31] Comments from Dr. David Kilcullen’s speech at Command and Staff College, MCU, 24 February 2012.

[32] Neilson, R. (Ed.). (1997) Sun Tzu and information warfare, National Defense University Press, Washington, D.C., 1997. p. 4

[33] Headquarters U.S. Marine Corps. *Marine Corps Planning Process.* MCWP 5-1. (Washington, DC: Headquarters U.S. Marine Corps, August 24, 2010), B-1

[34] Mapping the Information Environment**,** *By Robert Cordray III, Marc J. Romanych, Major, USA (Retired)*, 10.

[35] Headquarters U.S. Marine Corps. *Warfighting.* MCDP 1 (Washington, DC: Headquarters U.S. Marine Corps, June 30, 1991), 73.

[36] Sun Tzu, *The Art of War,* ed. Samuel B. Griffith, trans by Samuel B. Griffith, (New York: Oxford, 1963), 57